

WHAT IS CLAIMED IS:

1. A method that ensures policy coherence among a group of peer devices, comprising:
 - detecting an addition of a new policy version;
 - generating a message containing the newly added policy version; and
 - transferring the message to the peer devices.
2. The method of claim 1 wherein the newly added policy version is a policy that relates to at least one of system administration, system security, command and control, and courses of action.
3. The method of claim 1 further comprising:
 - determining whether a policy version has become newly active;
 - generating a second message containing an indication of the newly active policy version; and
 - sending the second message to the peer devices.
4. The method of claim 3 further comprising:
 - storing, in response to a policy version becoming newly active, an identifier of the newly active policy in an active policy database, the active policy database storing a list of active policy identifiers.

5. A system that ensures policy coherence among a group of peer devices,
comprising:

means for detecting an addition of one or more new policy versions;

means for generating a message containing the newly added one or more

5 policy versions; and

means for transferring the message to the peer devices.

6. A computer-readable medium containing instructions for controlling at
least one processor to perform a method that ensures policy coherence among a group of
peer devices, the method comprising:

determining whether a policy has been added;

5 generating, in response to a policy being added, a message containing the
added policy; and

sending the message to the peer devices.

7. The computer-readable medium of claim 6 wherein the method further
comprises:

determining whether a version of one of a group of policies has become
active;

5 generating a second message containing the active version;

transferring the second message to the peer devices.

8. The computer-readable medium of claim 7 wherein the method further comprises:

storing an identifier of the newly active policy in an active policy database, the active policy database including a list of active policy identifiers.

9. A policy server comprising:

a memory configured to store instructions; and

a processor configured to execute the instructions to determine whether one or more policy versions have been added, generate, in response to a policy version being added, a message containing the added policy version, and transfer the message to a group of peer devices.

10. The policy server of claim 9 wherein the processor is further configured to:

detect a policy version becoming newly active,

generate, in response to the detecting, a second message containing the newly active policy version, and

transmit the second message to the group of peer devices.

11. The policy server of claim 10 wherein the memory is further configured to:

store an active policy database containing a list of identifiers of active policies.

13. A method for distributing policies in a network having at least one anonymous policy server and at least one anonymous peer device, comprising:

- requesting a policy from the anonymous policy server;
- determining, via the anonymous policy server, whether an active version of the policy exists; and
- transferring, when an active version of the policy is determined to exist, the active policy version from the anonymous policy server to the anonymous peer device.

15. The method of claim 14 wherein the determining includes:

comparing the identifier in the policy request to a list of active policy identifiers.

16. The method of claim 13 further comprising:
- receiving, via the anonymous peer device, a policy;
 - determining whether the received policy is the requested policy;
 - discarding the received policy when the received policy is not the requested policy; and
 - implementing the received policy when the received policy is the requested policy.

17. A network comprising:
- at least one anonymous peer device configured to:
 - request a policy from at least one anonymous policy server,
 - determine whether a received policy is of a desired policy class,
 - and
 - implement the received policy when the received policy is an active policy of the desired policy class; and
 - at least one anonymous policy server configured to:
 - receive the request from the at least one anonymous peer device,
 - determine whether any version of the policy requested exists, and

transfer all versions of the policy to the peer device, indicating the active version, if any version is determined to exist.

18. The network of claim 17 wherein the at least one anonymous peer device is further configured to:

discard the received policy when the received policy is not of the requested policy class.

19. The network of claim 17 wherein, when requesting, the at least one anonymous peer device is configured to:

generate a policy request, the policy request containing an identifier that identifies the requested policy, and

5 transfer the policy request to the at least one anonymous policy server.

20. The network of claim 18 wherein, when determining, the at least one anonymous policy server is configured to:

compare the identifier in the policy request to a list of active policy identifiers.

21. A computer-readable medium containing instructions for controlling at least one processor to perform a method that distributes policies in a network having a policy server and a peer device, the method comprising:

5 to the peer device;

transferring, when an active version of at least one of the policies exists,

22. A computer-readable medium having a database structure comprising:

a version field that stores an identifier of a policy version; and

23. A computer-readable medium having a database structure comprising:

a version field that stores an identifier of an active policy version.

24. A method for implementing policies, comprising:

receiving a message, the message containing an identifier and one or more versions of a policy;

determining whether the identifier is in a list of policy identifiers;

5 discarding the message when the identifier is absent from the list; and

implementing an active version of the one or more policies when the identifier is present in the list.

**PATENT
DOCKET NO. 00-4007**

5 message containing an identifier and one or more versions of a policy, compare the identifier to the list of policy identifiers, discard the message when the identifier does not match a policy identifier in the list, and implement an active version of the policy when the identifier matches a policy identifier in the list.

sub
A1 7

[illegible]